UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/782,396	02/18/2004	Sourabh Satish	68865.001205	4350

69417 7590 07/06/2010

HUNTON & WILLIAMS LLP / SYMANTEC CORPORATION
INTELLECTUAL PROPERTY DEPT.
1900 K STREET, NW
SUITE 1200
WASHINGTON, DC 20006-1109

EXAMINER	
CALLAHAN, PAUL E	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
07/06/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/782,396	SATISH, SOURABH	
	Examiner	Art Unit	
	PAUL CALLAHAN	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 April 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,7-18 and 29-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 7-18 and 29-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application.
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is prompted by the Applicant's response filed 4-22-2010. Claims 1-4, 7-18 and 29-38 are pending and have been examined.

Response to Arguments

2. Applicant's arguments with respect to claims 1-4, 7-18 and 29-38 have been considered but are moot in view of the new ground(s) of rejection.

3. The previously indicated allowability of claims 5 and 6 is withdrawn in view of the newly discovered reference to Ko et al. Rejections based on the newly cited reference follow.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claim 38 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The preamble of claim 38 indicates that it is directed towards a computer program product, i.e., software. However, the claim does not positively recite any limitation that specifies the software as being embodied in a *non-transitory* computer

readable medium. Therefore, the claim sets forth only functional descriptive language and is non-statutory since this does not fall into one of the classes of invention eligible for the grant of a US patent. The most recent guidance received from the Office indicates that, unless software is embodied in a *non-transitory* computer-readable medium, the software in and of itself cannot be considered as a computer component, and hence cannot effect a change of state of a processor to produce a useful or tangible result.

The Examiner recommends that the claim be amended to indicate that the computer program product is embodied in a non-transitory computer-readable medium.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-4, 18, 37 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg US 6,357,008 and Ko et al., "Automated Detection of Vulnerabilities in Privileged Programs by Execution Monitoring", Proceedings of the 10th Annual Computer Security Applications Conference, Orlando, Florida, 1994 pages 134-144, (found at >http://seclab.cs.ucdavis.edu/papers.html<).

As for claim 1, Nachenberg teaches a method for providing computer security (abstract), comprising: determining, using a processor, whether an executable associated with a static state meets one or more first predetermined criteria (col. 14 lines 11-22: the exploration module evaluates an executable according to predetermined criteria of whether an emulated instruction matches an entry from a list of suspicious operations); associating a first risk level with the executable based at least in part upon whether the executable meets the one or more first predetermined criteria (col. 14 line 16: exploration module records the suspicious operation); determining whether a current process associated with the executable meets one or more second predetermined criteria (col. 15 line 49 through col. 17 line 21: the evaluation module examines the processes recorded by the exploration module during emulation. This emulation of code reads on a current process. The evaluation module uses a list of known suspicious operations to examine the operations noted by the exploration module, this reads on the use of a second predetermined criteria) ; associating a second risk level with the current process based at least in part upon whether the current process meets the one or more second predetermined criteria (col. 16 line 65 through col. 17 line 55: a second predetermined criteria includes a predetermined list of highly suspicious behaviors), wherein the current process is initially associated with the first risk level (col. 15 line 49 through col. 17 line 21: the evaluation module examines the processes recorded by the exploration module during emulation to which the first risk level has been assigned), and wherein the first risk level is updated to the second risk level for the current process based at least in part

upon whether the current process meets the one or more second predetermined criteria (col. 17 lines 12-55); and performing a predetermined responsive action with respect to the process if the second risk level exceeds a threat detection threshold (col. 17 lines 12-21, col. 17 lines 50-55); wherein determining whether the executable meets the one or more predetermined criteria does not comprise comparing the executable with a virus signature (Nachenberg discloses the use of emulation of code and the evaluation of code segments for suspicious behaviors and does not utilize virus signature matching). Nachenberg does not explicitly teach a step wherein the one or more first predetermined criteria allow a determination of at least one of: whether the executable is configured as a service and whether the executable is configured to run under a highly privileged account. However, Ko does teach these features (Introduction, Sec. 3.1 The Scope of Privileged Program Execution, Sec. 5 Real Time Security Monitoring, Sec. 6.3 Send Mail). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate this feature into the system of Nachenberg. It would have been obvious to do so since this would allow for the evaluation of executable in the system of Nachenberg where the monitoring is targeted to critical programs such as those operating under a highly privileged account.

As for claims 37 and 38: Claim 37 represents the apparatus configured to carry out the method steps of claim 1, Claim 38 represents the computer-program product that instructs a processor to undertake the method steps of claim 1. Claims 37 and 38

recite substantially the same limitations as claim 1 and are thereby rejected on the same basis as that claim.

As for claim 2, Nachenberg teaches the method for providing computer security of claim 1, wherein the risk level indicates a level of potential risk that will be brought by operating the executable (col. 17 lines 12-22).

As for claim 3, Nachenberg teaches the method for providing computer security of claim 1, wherein the risk level indicates how much risk the executable presents (col. 17 lines 12-22, lines 50-55: the evaluation module will report the type of virus likely present in the executable).

As for claim 4, Nachenberg teaches the method for providing computer security of claim 1, wherein the predetermined criterion includes a configuration criterion (col. 9 lines 52-62).

As for claim 18, Nachenberg teaches the method for providing computer security of claim 1 comprising associating with the executable, a risk type indicating a type of risk to which the executable is vulnerable (col. 17 lines 12-22, lines 50-55: evaluation module will report the type of virus likely present in the executable).

8. Claims 7, 8, 10, 12-17 and 29-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg and Ko, and further in view of Tajalli et al. (US 2004/0143749 A1).

As for claim 7, Nachenberg and Ko disclose all of the limitations of claim 7, except where the predetermined criterion is used to determine whether the executable is installed via a standard procedure. The general concept of determining whether an executable is installed via standard procedure is well known in the art as illustrated by Tajalli, who discloses controlling access to system resources by a process based on a behavior control description for the process set to which it belongs (Para. 0020, lines 5-7). Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Nachenberg and Ko to include the use of a predetermined criterion to determine if an executable has not properly installed, in order to prevent malicious code execution on a computer system.

As for claim 8, Nachenberg and Ko disclose all the limitations of claim 8, except where the predetermined criterion is used to determine whether the executable has sufficient access control. The general concept of determining if an executable has sufficient access control is well known in the art as illustrated by Tajalli, who discloses an access control engine used to monitor access to and use of critical system

resources: the IDS of Tajalli watches applications requested and resources used, looking for requests or uses that depart from acceptable use and behavior (Para. 0081, lines 1-11; Para. 0161, lines 12-14; Para. 0175, lines 5-6). Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Nachenberg and Ko to include the use of determining sufficient access control in order to control access rights to system resources.

As for claim 10, Nachenberg and Ko disclose all the limitations of claim 10, except the method of providing computer security wherein the predetermined criterion is used to determine whether the executable is signed. The general concept of determining if an executable is signed is well known in the art as illustrated by Tajalli, who discloses that the IDS will check for encryption within the executable (Para. 0161, lines 12-14; Para. 0169, line 1). Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Nachenberg and Ko to include the use of the step of determining if an executable is signed in order to determine the origin of the executable, as public key cryptography binds the signer's identity to the key used in signing.

As for claim 12, Nachenberg and Ko disclose all the limitations of claim 12 except providing computer security wherein the predetermined criterion includes a capability criterion. The general concept of a predetermined criterion that includes a capability

criterion is well known in the art as illustrated by Tajalli, who discloses a predetermined criterion including a capability criterion (Para. 0055, lines 1-2; Para. 0175, lines 5-6). Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Nachenberg and Ko to include the use of a capability criterion, since such would increase the ability of the system to protect against attack by malicious code.

As for claim 13, Nachenberg and Ko disclose all the limitations of the claim except the method for providing computer security wherein the predetermined criterion is used to determine whether the executable has networking capability. The general concept of determining if an executable has networking capability is well known in the art as disclosed by Tajalli (Para. 0244, lines 1; 0251, lines 2-9; Para. 0175, lines 5-6). Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Nachenberg and Ko to include the use of determining if malicious code has networking capability in order to protect against malicious code that may cause damage to a network.

As for claim 14, Nachenberg and Ko disclose all the limitations of claim 14 except the where the predetermined criterion is used to monitor whether the executable has privilege manipulation capability. The general concept of determining whether an executable has privilege manipulation capability is well known in the art as illustrated by

Tajalli (Para. 0050, lines 1-8:IDS would defines modifying or manipulating registry keys as inappropriate behavior to be blocked). Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Nachenberg and Ko to include the use of this step in order to protect the system against malicious codes that may act to modify a system registry for example.

As for claim 15, Nachenberg and Ko disclose all the limitations of claim 15 except the step wherein the predetermined criterion is used to determine whether the executable has remote process capability. The general concept of determining if an executable has remote process capability is well known in the art as illustrated by Tajalli, (Para. 0236, lines 1-3; Para. 0239, line 1: IDS is configured to control network services to include remote connection). Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Nachenberg and Ko to include the use of this step in order to prevent the network from being compromised by use a malicious code at a local site that allows unauthorized entry to the network from a remote location.

As for claim 16, Nachenberg and Ko disclose all the limitations of claim 16 except the step wherein the predetermined criterion is used to determine whether the executable has process launching capability. The general concept of determining if an executable code has process launching capability is well known in the art as illustrated

by Tajalli, (Para. 0244, lines 1-2; Para. 0249, lines 1-2: malicious code can initiate HTTP connection to other Web servers). Therefore, it would have been obvious for one ordinary skill in the art at the time of the invention to modify Nachenberg and Ko to include the step of determining if an executable code has process launching capability in order to stop malicious code from utilizing other system resources from the network.

As for claim 17, Nachenberg and Ko disclose all the limitation of the claim except the step wherein the predetermined criterion is used to determine whether the executable has a secure algorithm. The general concept of determining if malicious code has a secure algorithm is well known in the art as illustrated by Tajalli (Para. 0217, lines 1-2; Para. 0222, line 1: IDS controls access to any attributes of files or directories including if encryption is present for the executable). Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Nachenberg and Ko to include the use of this step in order to protect against executable code that uses encryption to hide a viral payload from a virus scanning routine.

As for claims 29-31, Nachenberg and Ko disclose all the limitation of the claims except the steps comprising analyzing historical evidence; records of activities, and log files. The general concept of analyzing historical evidence, activities records, and log files is well known in the art as illustrated by Tajalli (Para. 0091, lines 1-7; Para 0097, line 1). Therefore, it would have been obvious for one of ordinary skill in the art at the

time of the invention to modify Nachenberg and Ko to include the use of these steps in order to more effectively evaluate potentially malicious code by the use of records associated with past examples of such code.

As for claim 32, Nachenberg and Ko disclose all the limitations of the claim except the step wherein the historical evidence includes a system optimization file. The general concept of the use historical evidence that includes a system optimization file is well known in the art as illustrated by Tajalli (Para 0090, lines 3-8: system optimization files or swap files reside on the disk such that a communication module may retrieve this data and request an alert when an unusual event occurs). Therefore, it would have been obvious for one of ordinary skill in that art at the time of the invention to modify Nachenberg and Ko to include the use of swap files in order to obtain information relevant to building a system wide security policy.

As for claims 33 and 34, Nachenberg and Ko disclose all the limitation of the claims except the step of providing computer security wherein the historical evidence includes a crash dump. The general concept where such historical evidence includes a crash dump is well known in the art as illustrated by Tajalli (Para. 0090, lines 3-8: a communication module that monitors local log files, transfers log data to a management infrastructure, and request alerts when unusual events occur). Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to modify

Nachenberg and Ko to include the use a crash dump file and a prefetch file in order to gather information when system failures occur.

9. Claims 9, 11, 35, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg and Ko, and further in view of Khazan et al. (US 2005/0108562 A1).

As for claims 9 and 11, Nachenberg and Ko disclose all the limitations of the claims except where the predetermined criterion is used to determine whether the executable is recent and determine whether the executable has a modified date different from the created date. The general concept of determining whether an executable is recent and determining whether the executable has a modified date different from its creation date is well known in the art as illustrated by Khazan, who discloses analyzing an executable to determine when in time a modification has taken place (Para. 0107, lines 14; Para. 0115, lines 1-19). Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Nachenberg and Ko to include the use of this step in order to verify whether and when modification has taken place within an executable.

As for claims 35 and 36, Nachenberg and Ko disclose all the limitation of the claims except the steps of performing a dynamic risk analysis, and determining whether an action is required. The general concept of performing dynamic risk analysis and determining whether an action is required is well known in the art as illustrated by Khazan, who discloses a static and a dynamic analyzer (Para. 0040, lines 12-13); and determining whether an action is required (Para. 0099, lines 7-11, lines 21-26). Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Nachenberg and Ko to include the use of such a dynamic analyzer in order to determine whether an action is required since these steps would be useful in reducing system overhead during the evaluation of executables for malicious code.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/PEC/
AU2437

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2437